**SISTEMA Y SEGURIDAD DE USUARIO**

OBSERVACIONES: En la práctica se hace referencia al usuario sysadmin, este usuario deberá ser reemplazado por el que hayais creado en la instalación del sistema operativo por la contraseña que hayais puesto.

13.2.1 Paso 1

Las cuentas del usuario y del sistema se definen en los archivos /etc/passwd y /etc/shadow. Ver las primeras diez líneas del archivo /etc/passwd:

head /etc/passwd

Utiliza el comando grep para ver el registro de tu cuenta sysadmin:

grep sysadmin /etc/passwd

Otra forma de recuperar la información de la cuenta de un usuario es ejecutando el siguiente comando: getent passwd *username*. El comando getent tiene la ventaja sobre el comando grep, ya que también puede acceder a las cuentas de usuario que no están definidas localmente. En otras palabras, el comando getent puede obtener información sobre el usuario para los usuarios que se pueden definir en los servidores de directorio de red, tales como LDAP, NIS, el dominio de Windows, o los servidores de dominio de Active Directory.

Utiliza el comando getent para recuperar la información acerca del administrador de sistemas:

getent passwd sysadmin

## 13.2.4 Paso 4

Puedes ver la documentación de los campos en el archivo /etc/passwd con el siguiente comando:

man 5 passwd

Recuerda que mientras visualizas una página man, puedes presionar la tecla **Entrar** para moverte hacia adelante línea por línea, **Espacio** página por página y **q** para salir.

El archivo /etc/passwd tiene los siguientes campos delimitados por los dos puntos:

account:password:UID:GID:GECOS:directory:shell

Desglose de estos campos:

1. El campo de la cuenta es el nombre de usuario.
2. Este campo se utilizó originalmente para almacenar la contraseña, sin embargo, ahora normalmente la contraseña se almacena en el archivo etc/shadow. La x sirve como un indicador.
3. UID es el número de identificación del usuario.
4. GID es el número de identificación de grupo principal del usuario.
5. GECOS es el campo que normalmente se utiliza para almacenar el nombre completo del usuario.
6. El directorio es el directorio inicial («home») del usuario, donde se colocan después del primer registro en el sistema.
7. El campo shell define el shell tal como /bin/bash para un usuario normal, o /sbin/nologin para una cuenta que utiliza el sistema o un servicio.

## 13.2.5 Paso 5

Puedes consultar la información de la cuenta para tu cuenta, o una cuenta de usuario especificado, utilizando el comando id:

id id root

El archivo /etc/group, junto con /etc/passwd, determina tu pertenencia a grupos. Tu grupo principal predeterminado se determina haciendo coincidir tu GID ubicado en /etc/passwd con el GID definido para un grupo en el /etc/group. Cualquier pertenencias a grupos secundarios se definen en el archivo /etc/group.

El formato de las entradas en el archivo /etc/group para cada línea es:

group\_name:password:GID:user\_list

El comando getent puede recuperar información acerca de las entradas en el archivo /etc/group. Utiliza el comando getent para recuperar la información acerca de sysadmin y los grupos adm:

getent group sysadmin getent group adm

Los grupos se utilizan para controlar el acceso a los archivos.

Por defecto cualquier archivo nuevo que creas será propiedad de tu grupo primario. Para tener todos los archivos nuevos que creas en propiedad de uno de tus grupos secundarios, utiliza el comando el newgrp. El formato básico de este comando es *newgrpgroup\_name*. Tienes que ser miembro de un grupo para poder utilizar el comando newgrp. El comando id mostrará entonces ese *group\_name* como tu grupo principal.

Para cambiar la propiedad de grupo de uno de los archivos existentes que tu usuario posee, puedes utilizar el comando chgrp. El formato básico de este comando es chgrpgroup\_*name*file\_*name*.

Tienes ser miembro de un grupo para cambiar una propiedad de grupo de los archivos a ese grupo y tienes que poseer el archivo.

## 13.2.7 Paso 7

Dos comandos con salida sencilla para comprender de tu identidad son whoami y groups. El comando groups también se puede utilizar para obtener la lista de grupos para otro usuario. Utiliza el comando whoami y groups para tu cuenta y el comando groups para el usuario root:

whoami groups groups root

## 13.3 ¿Quién está en el Sistema?

En esta tarea vas a ejecutar algunos comandos para ver quién está registrado en el sistema.

## 13.3.1 Paso 1

Utiliza el comando who para obtener la lista actual de los usuarios en el sistema:

who

La salida del comando who tiene cuatro columnas:

**El nombre de usuario**: la primera columna muestra el nombre del usuario (sysadmin en el ejemplo anterior).

**La terminal**: la segunda columna muestra un identificador para un tipo de la terminal (tty en el ejemplo anterior). Cada terminal tiene un nombre que se utiliza por el superusuario para controlar los procesos.

**Fecha/hora**: la tercera columna es la fecha y hora en que se inició la sesión (Apr 11 14:32en la primera línea de salida en el ejemplo anterior).

**Host**: aunque no hay una salida para la cuarta columna en este caso, puede ser un nombre o una dirección IP de un host local o remoto. Las siguientes formas indican los inicios de sesión locales: (:#) o (:#.#).. De lo contrario, un host remoto se puede mostrar por nombre (si es resoluble) o por dirección IP.

Utiliza el comando w para obtener una visión más detallada de los usuarios que están actualmente en tu sistema:

w

Tu salida del comando w muestra:

## 13.4 El Usuario root

En esta tarea, aprenderás cómo acceder a la cuenta de usuario root en un par de maneras diferentes.

La cuenta del usuario root es especial en Linux, ya que tiene una cantidad prácticamente ilimitada de control y acceso al sistema. En realidad no es el nombre del usuario, pero el UID con un valor de cero que otorga esta autoridad.

En general, no se considera una buena práctica iniciar sesión en el sistema como usuario root. Esto es especialmente cierto en el entorno gráfico.

Para acceder a la cuenta de usuario root, normalmente se utilizan los comandos su o sudo.

El comando su por lo general se utiliza para cambiar de usuario para iniciar un nuevo shell como otro usuario; el valor predeterminado es el usuario root. El comando su se utiliza normalmente cuando necesitas ejecutar una serie de comando como usuario root.

El comando sudo se suele utilizar para ejecutar un solo comando como usuario root colocando el prefijo sudo a ese comando. El comando sudo debe ser configurado por el usuario root antes de que un usuario normal pueda utilizarlo.

## 13.4.1 Paso 1

Para configurar el comando sudo para los usuarios regulares, utiliza el comando visudo. Esto requiere acceso root ya que el comando visudo falla si lo ejecutan los usuarios regulares. Intenta configurar el acceso al comando sudo:

visudo

El resultado muestra que el comando visudo falla debido a que intentó modificar el archivo /etc/sudoers, un archivo que los usuarios normales no pueden modificar debido a los permisos. Este archivo controla el acceso al comando sudo y nunca debe ser modificado directamente, sino más bien con el comando visudo.

## 13.4.2 Paso 2

Cambia el usuario al usuario root y proporciona la contraseña root de netlab123 cuando se te solicite:

su - netlab123

El guión después del comando su es una abreviatura de la opción -l, que hace que la entrada realizada por su sea un inicio de sesión completo mediante la ejecución de los scripts de entrada que pertenecen al usuario root.

Sin -, o -l, el comando su cambiará tu identidad de usuario, pero no va a ejecutar las secuencias de comandos de inicio de sesión del nuevo usuario. Esto puede causar algunos problemas, sobre todo cuando se cambia a la cuenta root. En la mayoría de los casos cuando cambias de usuario, quieres llevar a cabo un inicio de sesión completo para que puedas inicializar las variables de entorno, las funciones y los alias que normalmente se inicializan para un usuario.

## 13.4.3 Paso 3

Ahora que ya estás en el sistema como usuario root, deberías poder ejecutar el comando para configurar el acceso sudo:

visudo

## 13.4.4 Paso 4

Para habilitar el acceso básico a la utilización del comando sudo, debes añadir una entrda al archivo /etc/sudoers que estás editando ahora. Ya que estás en el vi editor por defecto, escribe lo siguiente para encontrar esta entrada:

| **Qué escribir** | **Significado** |
| --- | --- |
| G | Ir al final del archivo |
| o | Abrir una nueva línea debajo del cursor |
| sysadmin ALL=(ALL) ALL | La entrada que permite al administrador de sistema acceder al sudo |
| **ESC** | La tecla **Escape** regresa al modo de comando |
| :wq | Guardar los cambios y salir |

Si introduces los datos al archivo correctamente, debes regresar al prompt de shell. Sin embargo, si al salir de la edición, se te presenta un mensaje que dice «What now», presiona **Entrar** para ver tus opciones. Se recomienda que escribas x para salir sin guardar los cambios en el archivo sudoers y repitas este paso.

## 13.4.5 Paso 5

Vuelve a la cuenta sysadmin para verificar que sudo proporciona acceso root escribiendo lo siguiente:

exit

## 13.4.6 Paso 6

Trata de ver las primeras líneas del archivo /etc/shadow, un archivo que contiene las contraseñas cifradas de los usuarios y la información sobre el su caducidad:

head -3 /etc/shadow

## 13.4.7 Paso 7

Ten en cuenta que los permisos en el archivo /etc/shadow indican que sólo los miembros del grupo shadow tienen permiso para ver el archivo:

ls -l /etc/shadow

Ten en cuenta que el usuario root puede ver cualquier archivo. Esto se debe a que la cuanta root tiene privilegios especiales que trascienden los permisos de archivos regulares.

## 13.4.8 Paso 8

Utiliza el comando sudo para ver las primeras líneas del archivo /etc/shadow:

sudo head -3 /etc/shadow (proporciona la contraseña del usuario sysadmin: netlab123)

Nota importante: La contraseña que proporcionaste era para tu cuenta sysadmin, no para la cuenta root. Una vez configurado el sudo para tu cuenta, no necesitas saber la contraseña root para ejecutar los comandos sudo como el usuario root.